# On the Security of Non-Linear HB (NLHB) Protocol Against Passive Attack

Mohammad Reza Sohizadeh Abyaneh*

**Abstract**. As a variant of the HB authentication protocol for RFID systems, which relies on the complexity of decoding *linear* codes against passive attacks, Madhavan et al. presented Non-Linear HB(NLHB) protocol. In contrast to HB, NLHB relies on the complexity of decoding a class of *non-linear* codes to render the passive attacks proposed against HB ineffective. Based on the fact that there has been no passive solution for the problem of decoding a random non-linear code, the authors have claimed that NLHB's security margin is very close to its key size.

In this paper, we show that passive attacks against HB protocol can still be applicable to NLHB and this protocol does not provide the desired security margin. In our attack, we first linearize the non-linear part of NLHB to obtain a *HB equivalent* for NLHB, and then exploit the passive attack techniques proposed for the HB to evaluate the security margin of NLHB. The results show that although NLHB's security margin is relatively higher than HB against similar passive attack techniques, it has been overestimated and, in contrary to what is claimed, NLHB is vulnerable to passive attacks against HB, especially when the noise vector in the protocol has a low weight.

**Key Words:** RFID, Authentication, LPN problem, HB protocols.

*Department of Informatics, University of Bergen

# 1 INTRODUCTION

Radio Frequency Identification (RFID) tags are forming the next generation technology for identifying objects, and are poised to supplant barcodes in near future. Their advantages such as: more storage and ease of use have caused a universal proliferation of RFID tags in many commercial as well as national security applications; [1] ranging from electronic passports [3, 4], contactless credit cards [2], to supply chain management [5–7].

This widespread deployment of RFID tags has raised some concerns about their security. On the other hand, RFID tag constraints in processing power and memory make them tougher to deal with in security. These kinds of constraints dictate a paradigm shift in security provision for RFIDs which is known as *lightweight cryptography*.

Lightweight authentication protocol is a subset of lightweight cryptography which tackles providing authentication in highly constrained environments (e.g RFID systems) as well as security provision to a reasonable extent [8, 9].

## 1.1 NOTATIONS

- $G_{a\times b}$: $a \times b$ binary matrix.
- $h_{1\times b}$: $1 \times b$ binary vector.
- $A \otimes B$: matrix multiplication of A and B.
- $\oplus$: XOR operation.
- $x_i$: $i^{th}$ bit of binary vector $x$.
- $Hwt(.)$: hamming weight function.
- $h \otimes G$: matrix multiplication of a vector $h$ into matrix $G$.
- $R, T$: *Reader* and *Tag* respectively.

## 1.2 HB FAMILY PROTOCOLS

The HB lightweight authentication protocol proposed by Hopper and Blum in 2001 [10] is the first in the *HB family* of protocols. An overview of a paralleled $r$-round of the HB protocol is given in Figure 1. This protocol aims at unilateral authenticating of an RFID tag to a reader

| **Specifications** |
| --- |
| $-r, \eta, \epsilon$:Public parameters. |
| $-\nu$ : $d$-bit noise vector where: $Prob(\nu_i = 1) = \eta, i = 1, ..., r$ |
| **HB Protocol** |
| - Secret parameter $x \in \{0,1\}^k$ is shared between $R$ and $T$. |
| (1) $R$ : Chooses a random $A_{k \times r}$ matrix. |
| (2) $R \Rightarrow T : A$ |
| (3) $T$ : Computes $z_{1 \times r} = (x \otimes A) \oplus \nu_{1 \times r}$ |
| (4) $T \Rightarrow R : z$ |
| (5) $R$ : ACCEPTS iff $Hwt(z \oplus (x \otimes A) \leq \epsilon r)$ |

**Fig. 1:** *Parallelized version of an r-round HB protocol*

only by lightweight operations. The operations used in this protocol are one matrix multiplication and some XORs. On the other hand, The security of this algorithm and some others in this family against passive attacks is reduced to a well-known NP-hard problem called *Learning with Parity Noise* (LPN) problem [11]. The other members of this family emerged as a result of proposing an attack on the previous one in order to eliminate the weaknesses and render the prior proposed attacks ineffective. Some of other members of this family are: $HB^+$ [12],$HB^{++}$ [13], HB* [14],HB-MP [16],$HB^\sharp$ [21] and NLHB [17]. Attacks which have targeted these authentication protocols consists both *passive* [18–20] and *active* types [21, 22]. In an active attack, the adversary is able to eavesdrop the transcripts between a reader and a tag as well as being able to interact with them and manipulate the messages exchanging in between [23] in order to impersonate either of them. It should be noted that active attacks involve a broad spectrum of attacks which differ in adversary's capabilities (e.g. DET [23] and GRS [21] attack models). On the contrary, in a passive attack, the adversary has only access to the transcripts from an arbitrary number of authentication sessions between a tag and a reader and aims at impersonating either of them.

### 1.3 LPN Problem

If we see from a passive adversary perspective, who has only access to $s$ number of parallelized $r$-round HB protocol transcripts(i.e. $A_{k \times n}, z_{1 \times n}, \eta$ where $n = s \times r$) and his goal is to recover secret parameter $x$, it will be obvious that she faces a decoding problem of a codeword $(x \otimes A)$

generated by a random linear block code $A$ in presence of noise $\nu$ [25]. This problem is called *LPN problem* with parameters $k, n, \eta$ and has been shown to be NP-hard in worst case [25].

## 1.4 LPN Solvers

In addition to worst case complexity results of the LPN problem, there are numerous studies on average case complexity [20, 26]. These studies has led to finding some algorithms to solve the LPN problem under certain assumptions(*LPN solvers*). Proposition of these algorithms paved the way for applying passive attack against some of HB family protocols.

In [20], the BKW algorithm has been reported which can be considered as an instance of the generalized birthday paradox [27]. In [18], another algorithm(FMICM) has been proposed inspired by fast correlation attack [24] on ciphers. The solution proposed by the FMICM algorithm is under the assumption of having low bit rate($\frac{k}{n}$)and high $\eta$. Besides some deterministic LPN solvers such as the two aforementioned algorithms, there are some probabilistic algorithms such as CTIN [19] which accomplish their goal even when the adversary has access to less amount of transcripts comparing to deterministic ones.

As said, applying any passive attack on HB protocol requires to utilize an LPN solver algorithm to solve the LPN problem. Thus, the terms *LPN solver* and *passive attack* against HB protocol point to the same notion and are used interchangeably hereafter.

Using LPN solvers caused a dramatic decrease in security margin of some of HB family protocols against passive attacks [18, 19]. As an attempt to search for a variant of the HB, which relies on the complexity of decoding *linear* codes against passive attacks, Madhavan et al. presented Non-Linear HB(NLHB) protocol. In contrast to HB, NLHB relies on the complexity of decoding a class of *non-linear* codes to render the passive attacks proposed against HB ineffective. Based on this fact that there has been no passive solution for the problem of decoding a random non-linear code, the authors have claimed that NLHB's security margin is very close to its key size.

**Our Contribution.** In this paper, we present a passive attack on the NLHB protocol. The idea of our attack is the linearization of the non-linear part of the NLHB protocol to convert it to an equivalent of conventional HB protocol. This method has been adopted in order to be able to deploy the passive attack techniques used against HB on NLHB.

| **Specifications** |
| --- |
| $-r, \eta, p, \epsilon$:Public parameters<br>$-d = r - p$<br>$-\nu$ : $d$-bit noise vector where: $Prob(\nu_i = 1) = \eta, i = 1, ..., d$ |
| **NLHB Protocol** |
| - Secret parameter $x \in \{0,1\}^k$ is shared between $R$ and $T$.<br>(1) $R$ : Chooses a random $A_{k \times r}$ matrix.<br>(2) $R \Rightarrow T : A$<br>(3) $T$ : Computes $z_{1 \times d} = f(x \otimes A) \oplus \nu_{1 \times d}$<br>(4) $T \Rightarrow R : z$<br>(5) $R$ : ACCEPTS iff $Hwt(z \oplus f(x \otimes A)) \leq \epsilon d$ |

**Fig. 2:** *Parallelized version of an r-round NLHB protocol*

**Outline.** The remainder of this paper is organized as follows. In Section 2, we give a brief description of the NLHB protocol and Section 3 elaborates on our attack method on it. In Section 4, we display the results of applying our attack on NLHB compared to similar attacks on HB and eventually, Section 5 concludes the paper.

## 2 Description of the NLHB Protocol

Figure 2 shows one session of a parallelized $r$-round version of NLHB protocol. The tag and reader share a $k$-bit secret $x$ in advance. The reader transmits a random $k \times r$ challenge matrix $A$ to the tag. Having $A$ received, the tag computes $f(x \otimes A)$. Subsequently, it also computes $z = f(x \otimes A) \oplus \nu$, where $\nu$ is a noise-vector whose bits are all independently distributed according to the Bernoulli distribution with parameter $\eta$, just like the noise vector in the HB protocol. $x \otimes A$ is also an $r$-bit vector similar to HB, but $z$ differs in size. It is a $d$-bit vector($d = r - p$). On receiving $z$, the reader checks whether $Hwt(z \oplus f(x \otimes A)) \leq \epsilon d$ Where $0 < \epsilon < \eta < 0.5$. If this is true, reader accepts and this means that the tag has been authenticated successfully.

### 2.1 Function $f$

The function $f$ used in the protocol is a non-linear function which maps $\{0,1\}^r$ to $\{0,1\}^d$. Specifically, in [17], the function $f$ is defined as

| p | g |
|---|---|
| 2 | $x_{i+1}x_{i+2}$ |
| 3 | $x_{i+1}x_{i+2} \oplus x_{i+1}x_{i+3}$ |
| | $x_{i+1}x_{i+3} \oplus x_{i+2}x_{i+3}$ |
| | $x_{i+1}x_{i+2} \oplus x_{i+2}x_{i+3} \oplus x_{i+3}x_{i+1}$ |
| 4 | $x_{i+1}x_{i+4} \oplus x_{i+2}x_{i+3}$ |
| | $x_{i+1}x_{i+4} \oplus x_{i+2}x_{i+4} \oplus x_{i+3}x_{i+4}$ |
| | $x_{i+1}x_{i+4} \oplus x_{i+2}x_{i+3} \oplus x_{i+3}x_{i+4}$ |

**Table 1:** *Proposed g function for NLHB protocol*

following:

$$y = f(x); y \in \{0,1\}^d, x \in \{0,1\}^r \tag{1}$$

and

$$y_i = x_i \oplus g(x_{i+1}, ..., x_{i+p}) \tag{2}$$

where $g : \{0,1\}^p \to \{0,1\}$ is a non linear boolean function. The authors have also proposed some specific functions for $g$ corresponding to parameter $p$ to achieve maximum entropy and lower the complexity of the protocol (see Table 1). In [17], the authors have shown that for a general function of $f$, the existing passive attacks on the HB protocol family (discussed in section 1.4) do not work on their protocol.

## 3 Proposed Attacking Method

### 3.1 Description

In this section, we present our three-phase passive attack on the NLHB protocol. In this passive attack, we assume that the attacker has access to $n$ rounnds of the NLHB protocol where $n = s \times r$ (i.e. $s$ sessions of an $r$-round protocol) and thus can form matrix $A$ according to (3).

$$A_{k\times n} = (A^1_{k\times r} || \dots || A^s_{k\times r}) \tag{3}$$

where $A^i_{k\times r}$ is random matrix in $i^{th}$ session.

Exploiting the passive attack techniques proposed for the HB protocol, we require to find an *HB equivalent* of the NLHB protocol. This implies that we should first find a linear approximation of its non-linear part and then update its parameters accordingly. Hence, phase I and II of

| p | g | $\approx$ g | q |
|---|---|---|---|
| 2 | $x_{i+1}x_{i+2}$ | $x_{i+1}$ | 0.75 |
| | | $x_{i+2}$ | 0.75 |
| 3 | $x_{i+1}x_{i+2} \oplus x_{i+1}x_{i+3}$ | $x_{i+1}$ | 0.75 |
| | $x_{i+1}x_{i+3} \oplus x_{i+2}x_{i+3}$ | $x_{i+3}$ | 0.75 |
| | $x_{i+1}x_{i+2} \oplus x_{i+2}x_{i+3} \oplus x_{i+3}x_{i+1}$ | $x_{i+2}$ | 0.75 |
| 4 | $x_{i+1}x_{i+4} \oplus x_{i+2}x_{i+3}$ | $x_{i+1}$ | 0.62 |
| | $x_{i+1}x_{i+4} \oplus x_{i+2}x_{i+4} \oplus x_{i+3}x_{i+4}$ | $x_{i+4}$ | 0.75 |
| | $x_{i+1}x_{i+4} \oplus x_{i+2}x_{i+3} \oplus x_{i+3}x_{i+4}$ | $x_{i+2} \oplus x_{i+3} \oplus x_{i+4} \oplus 1$ | 0.75 |

**Table 2:** *Best linear approximation of function g in NLHB protocol and their probabilities*

our attack tackle the former and latter implications and phase III is the utilization of passive attack techniques on the equivalent HB protocol.

**Phase I: Linearization**

Our objective in this phase is to find a relatively good linear approximation for non-linear part of NLHB to convert the problem of decoding a non-linear random code to LPN problem. To do so, we should find a matrix $B$ such that the probability $q$ in (4) is relatively high.

$$prob(f\,(x \otimes A) = (x \otimes A)_{1\times n} \otimes B_{n\times n^*}) = q; \;\; n^* = n - s \times p \quad (4)$$

To construct matrix $B$, we require to linearize the whole system and according to (2), the non-linear part of the algorithm is the function $g$ which will be our target for linearization hereafter. We can use the Walsh-Hadamard technique [28] to find the best linear approximation for the boolean function $g$ such that:

$$g(x_{i+1}, ..., x_{i+p}) \approx \sum_{j=i+1}^{i+p} c_j x_j \quad (5)$$

According to Table 2, all functions proposed for NLHB can be linearly approximated with a relatively high probability. A linear approximation of all $g$ functions with their probabilities $q$ are shown in Table 2. Having $c_j$s from linear approximation of $g$, we can conclude this phase by calculating matrix $B$. Similar to matrix $A$ in (3), matrix $B$ for $s$ sessions has the following structure:

$$B_{n\times n^*} = (B^1_{n\times d}||\ldots||B^s_{n\times d}) \quad (6)$$

in which,

$$b_{ij}^{l} = \begin{cases} 1 & \text{if } i = j \\ c_j & \text{for } j = i+1, ..., i+p \\ 0 & \text{otherwise} \end{cases} \tag{7}$$

where $i = 1, ..., n;\ j = 1, ..., n^*;\ l = 1, ..., s$ or,

$$B_{n\times d}^{l} = \begin{pmatrix} 1 & 0 & & 0 \\ c_1 & 1 & & 0 \\ c_2 & c_1 & & 0 \\ \vdots & c_2 & & \vdots \\ c_p & \vdots & \dots & \\ 0 & c_p & & 0 \\ 0 & 0 & & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & & c_p \end{pmatrix};\ l = 1, ..., s \tag{8}$$

**Phase II: Finding a new linear equivalent protocol**
In this phase, we attempt to find an equivalent HB protocol for NLHB using the linear approximation obtained in previous phase. Since our approximation is valid with probability $q$, we can rewrite (4) as following to formulate the HB equivalent of our NLHB protocol with new parameters denoted by $^*$.

$$\begin{aligned} y &= f(xA) = (x \otimes A) \otimes B \oplus e \\ &= (x \otimes A^*) \oplus e \end{aligned} \tag{9}$$

where:

$$\begin{aligned} A^*_{k\times n^*} &= A_{k\times n} \otimes B_{n\times n^*} \\ Prob(e_i = 1) &= (1-q);\ i = 1, ..., n^* \end{aligned} \tag{10}$$

Now, by adding the noise of protocol to both side of (9) we have:

$$y = f(x \otimes A) \oplus \nu = (x \otimes A^*) \oplus \nu \oplus e = (x \otimes A^*) \oplus \nu^* \tag{11}$$

where $\nu^* = \nu \oplus e$.

As $\nu$ and $e$ are independent, the probability of error for the new noise vector can be calculated by (12).

$$\begin{aligned} Prob(\nu_i^* = 1) = \eta^* = Prob(\nu_i = 1) + Prob(e_i = 1) - \\ Prob(\nu_i = 1) \times Prob(e_i = 1) \\ = \eta + (1-q) - (1-q)\eta. \end{aligned} \tag{12}$$

As it is apparent from (12), the noise of the equivalent HB protocol($\nu^*$) is more than the noise in NLHB protocol. Therefore, in general, the NLHB protocol is more resistant against the passive attacks comparing to the HB protocol with the same parameters. Nevertheless, according to our results in Section 4, this strength is far lower than it has been claimed and desired.

**Phase III: Recovering secret parameter** $x$

Up to here, we have accomplished to find an equivalent HB form for the NLHB protocol. From now on, the problem of recovering secret parameter $x$ is an LPN problem with random matrix $A^*$ and parameters $k, n^*, \eta^*$ (equivalent HB parameters) and therefore can be achieved by using any of LPN solvers discussed in Section 1.4.

### 3.2 Complexity of the Attack

Complexity of our attack consists of three parts corresponding to each phase. For phase I, we need to find the best linear approximation for boolean function $g$ with $p$ variables. This can be done by finding Walsh-Hadamard coefficients of $g$ with complexity of $O(p2^p)$. In phase II, we just have a matrix multiplication of $A_{k\times n}$ and $B_{n\times n^*}$ to form $A^*$. This process has the compexity of $O(knn^*)$ in general. But due to sparse form of matrix $B$ in (8), this complexity is reduced to $O(kpn^*)$. Finally, the complexity of phase III relies on the complexity of the LPN solver algorithm. So, the complexity of our attack is calculated by (13) in which the complexity of phases I, II and III are denoted by $C_I, C_{II}$ and $C_{III}$ respectively.

$$C = C_I + C_{II} + C_{III} = O(p2^p) + O(kpn^*) + C_{III} \approx O(kpn^*) + C_{III}, n^* >> p \quad (13)$$

It should be noted that the complexity which computed in(13) is the *time complexity* of our attack. To be more precise, we should calculate the *data complexity* of our attack in terms of the amount of protocol rounds required to apply the attack($n^*$) as well. Phase I and II are applied on the number of rounds of the protocol which are determined in phase III and these two phases do not impose any additional data complexity to our attack. Therefore, data complexity of our attack only relies on the data complexity of LPN solvers discussed in [18–20].

## 4 RESULTS

In this section, we demonstrate the results of applying our passive attack using three LPN solvers BKW,FMICM and CTIN on NLHB and compare the security margins of NLHB(i.e. its equivalent HB) with HB protocol with the same parameters. Our motivation to do such an unfair comparison is to demonstrate that security margin of the NLHB is not far more than th HB protocol with the same parameters.

Tables 3, 4 and 5 show a comparative time and data complexity of applying passive attacks on NLHB and HB protocol for three different but low noise probability ($\eta = 0.15, 0.10, 0.05$ for HB and correspondent $\eta^* = 0.36, 0.32, 0.29$ in NLHB respectively) as well as the number of rounds of the protocol required to apply the attack (data complexity). As the results show, not only are the passive attacks on HB applicable to NLHB, but also the security margin of NLHB protocol is not far more than HB protocol. It is manifest that the results of our attack using FMICM are remarkably better in comparison with BKW and CTIN. Furthermore, we can have better results when the noise vector in the protocol has a lower weights(Table 5).

## 5 CONCLUSIONS

We presented a passive attack against NLHB protocol by finding an HB equivalent of it and then using some LPN solver techniques. Our results not only negate the authors claim that their protocol is resistant to passive attacks on the HB protocol but also show that the NLHB has not elevated the security margin of the HB remarkably and this is mainly due to the poor design of the non-linear part of the NLHB.

In summary, what we did is as follows. We:

- targeted Non-Linear HB protocol for passive attack.
- found a linear approximation of the non linear part of the protocol and converted the protocol to an equivalent HB protocol with higher noise.
- applied three well-known LPN solver techniques as a passive attack to the equivalent protocol.
- calculated the complexity of our attack on NLHB.

| **Key Length** | **Time Complexity** | | | | | | **Data Complexity** | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | **CTIN** | | **BKW** | | **FMICM** | | **CTIN** | | **BKW** | | **FMICM** | |
| | HB | NLHB | HB | NLHB | HB | NLHB | HB | NLHB | HB | NLHB | HB | NLHB |
| 32 | $2^{21}$ | $2^{26}$ | $2^{3}$ | $2^{15}$ | $2^{8}$ | $2^{12}$ | $2^{3}$ | $2^{11}$ | $2^{3}$ | $2^{15}$ | $2^{8}$ | $2^{12}$ |
| 64 | $2^{9}$ | $2^{36}$ | $2^{31}$ | $2^{40}$ | $2^{19}$ | $2^{22}$ | $2^{13}$ | $2^{14}$ | $2^{31}$ | $2^{40}$ | $2^{19}$ | $2^{22}$ |
| 128 | $2^{23}$ | $2^{78}$ | $2^{47}$ | $2^{62}$ | $2^{35}$ | $2^{45}$ | $2^{13}$ | $2^{15}$ | $2^{47}$ | $2^{62}$ | $2^{35}$ | $2^{45}$ |
| 192 | $2^{39}$ | $2^{118}$ | $2^{63}$ | $2^{83}$ | $2^{52}$ | $2^{67}$ | $2^{13}$ | $2^{16}$ | $2^{63}$ | $2^{83}$ | $2^{52}$ | $2^{67}$ |
| 256 | $2^{56}$ | $2^{162}$ | $2^{76}$ | $2^{99}$ | $2^{71}$ | $2^{88}$ | $2^{14}$ | $2^{16}$ | $2^{76}$ | $2^{99}$ | $2^{71}$ | $2^{88}$ |

**Table 3.** Time complexity and Data complexity passive attacks on HB and NLHB $\eta = 0.15$,$\eta^* = 0.36$

| **Key Length** | **Time Complexity** | | | | | | **Data Complexity** | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | **CTIN** | | **BKW** | | **FMICM** | | **CTIN** | | **BKW** | | **FMICM** | |
| | HB | NLHB | HB | NLHB | HB | NLHB | HB | NLHB | HB | NLHB | HB | NLHB |
| 32 | $2^{1}$ | $2^{13}$ | $2^{20}$ | $2^{25}$ | $2^{8}$ | $2^{10}$ | $2^{10}$ | $2^{13}$ | $2^{20}$ | $2^{25}$ | $2^{8}$ | $2^{10}$ |
| 64 | $2^{4}$ | $2^{30}$ | $2^{28}$ | $2^{37}$ | $2^{17}$ | $2^{19}$ | $2^{10}$ | $2^{13}$ | $2^{28}$ | $2^{37}$ | $2^{17}$ | $2^{19}$ |
| 128 | $2^{13}$ | $2^{66}$ | $2^{44}$ | $2^{59}$ | $2^{35}$ | $2^{38}$ | $2^{13}$ | $2^{15}$ | $2^{44}$ | $2^{59}$ | $2^{35}$ | $2^{38}$ |
| 192 | $2^{24}$ | $2^{102}$ | $2^{57}$ | $2^{78}$ | $2^{54}$ | $2^{63}$ | $2^{13}$ | $2^{15}$ | $2^{57}$ | $2^{78}$ | $2^{54}$ | $2^{63}$ |
| 256 | $2^{31}$ | $2^{140}$ | $2^{70}$ | $2^{94}$ | $2^{71}$ | $2^{85}$ | $2^{14}$ | $2^{16}$ | $2^{70}$ | $2^{94}$ | $2^{71}$ | $2^{85}$ |

**Table 4.** Time complexity and Data complexity passive attacks on HB and NLHB $\eta = 0.1$,$\eta^* = 0.32$

| **Key Length** | **Time Complexity** | | | | | | **Data Complexity** | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | **CTIN** | | **BKW** | | **FMICM** | | **CTIN** | | **BKW** | | **FMICM** | |
| | HB | NLHB | HB | NLHB | HB | NLHB | HB | NLHB | HB | NLHB | HB | NLHB |
| 32 | $2^{1}$ | $2^{10}$ | $2^{17}$ | $2^{23}$ | $2^{6}$ | $2^{8}$ | $2^{11}$ | $2^{13}$ | $2^{17}$ | $2^{23}$ | $2^{6}$ | $2^{8}$ |
| 64 | $2^{2}$ | $2^{26}$ | $2^{24}$ | $2^{35}$ | $2^{12}$ | $2^{16}$ | $2^{11}$ | $2^{13}$ | $2^{24}$ | $2^{35}$ | $2^{12}$ | $2^{16}$ |
| 128 | $2^{5}$ | $2^{57}$ | $2^{37}$ | $2^{57}$ | $2^{25}$ | $2^{36}$ | $2^{14}$ | $2^{15}$ | $2^{37}$ | $2^{57}$ | $2^{25}$ | $2^{36}$ |
| 192 | $2^{9}$ | $2^{88}$ | $2^{50}$ | $2^{73}$ | $2^{42}$ | $2^{54}$ | $2^{14}$ | $2^{16}$ | $2^{50}$ | $2^{73}$ | $2^{42}$ | $2^{54}$ |
| 256 | $2^{14}$ | $2^{120}$ | $2^{60}$ | $2^{89}$ | $2^{58}$ | $2^{76}$ | $2^{14}$ | $2^{16}$ | $2^{60}$ | $2^{89}$ | $2^{58}$ | $2^{76}$ |

**Table 5.** Time complexity and Data complexity passive attacks on HB and NLHB $\eta = 0.05$,$\eta^* = 0.29$

## 6 ACKNOWLEDGEMENTS

We would like to thank prof. Øyvind Ytrehus for his review and helpful comments to improve our manuscript. We also appreciate anonymous reviewers' time and their valuable feedbacks.

## REFERENCES

[1] Raphael C.-W. Phan: *Cryptanalysis of a New Ulteralightweight RFID Authentication Protocol-SASI*, IEEE Transaction on Dependable and Secure Computing, 2008.

[2] T.S. Heydt-Benjamin, D.V. Bailey, K. Fu, A. Juels, and T. O'Hare: Vulnerabilities in First-Generation RFID-Enabled Credit Cards, Proc. 11th Int'l Conf. Financial Cryptography and Data Security (FC '07), pp. 2–14, 2007.

[3] D.Carluccio, K.Lemke, C.Paar: E-passport:*the Global Traceability or How to feel like a UPS package*, Proceeding of WISA'06, LNCS 4298, Springer, pp.391–404, 2007.

[4] J.-H. Hoepman, E. Hubbers, B. Jacobs, M. Oostdijk, and R.W. Schreur, Crossing Borders: *Security and Privacy Issues of the European e-Passport*, Proc. First Int'l Workshop Security (IWSEC '06), pp.152–167,2006.

[5] CASPIAN, Boycott Benetton: http://www.boycottbenetton.com,2007.

[6] Mitsubishi Electric Asia Switches on RFID: www.rfidjournal.com/article/articleview/2644/,2006.

[7] Target, Wal-Mart Share EPC Data: http://www.rfidjournal.com/article/articleview/642/1/1/,2005.

[8] G. Avoine and P. Oechslin. *RFID Traceability: A Multilayer Problem*, Financial Cryptography - FC'05, LNCS, Springer, 2005.

[9] T. Dimitriou. *A Lightweight RFID Protocol to Protect Against Traceability and Cloning Attacks*,Proceedings of the IEEE International Conference on Security and Privacy for Emerging Areas in Communication Networks, SECURECOMM, 2005.

[10] N.J. Hopper and M. Blum. *Secure Human Identifcation Protocols*, in C. Boyd (ed.) Advances in Cryptology - ASIACRYPT 2001, Volume

2248, Lecture Notes in Computer Science, pp. 52–66, Springer-Verlag, 2001.

[11] J. Bringer, H. Chabanne, and E. Dottax. *HB++: a Lightweight Authentication Protocol Secure Against Some Attacks*, IEEE International Conference on Pervasive Services, Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing SecPerU, 2006.

[12] Julien Bringer and Herve Chabanne. *Trusted-HB: a low-cost version of HB+ secure against man-in-the-middle attacks*. CoRR, abs/0802.0603, 2008.

[13] Julien Bringer, Herve Chabanne, and Emmanuelle Dottax. *HB++: a lightweight authentication protocol secure against some attacks*. In Second International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing (SecPerU 2006), 29 June 2006, Lyon, France, pages 28–33. IEEE Computer Society, 2006.

[14] Dang Nguyen Duc and Kwangjo Kim. *Securing HB+ against GRS man-in-the-middle attack*. In Institute of Electronics, Information and Communication Engineers, Symposium on Cryptography and Information Security, 2007.

[15] Henri Gilbert, Matthew J. B. Robshaw, and Yannick Seurin. *HB♯: Increasing the security and effciency of HB+*. Advances in Cryptology EUROCRYPT 2008, 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Istanbul, Turkey, April 13–17, 2008. Proceedings, volume 4965 of Lecture Notes in Computer Science, pages 361–378.Springer, 2008.

[16] J. Munilla and A. Peinado. *HB-MP: A further step in the HB-family of lightweight authentication protocols.* Computer Networks, 2007.

[17] Mukundan Madhavan,Andrew Thangaraj,Yogesh Sankarasubramaniam and Kapali Viswanathan,*NLHB : A Non-Linear Hopper Blum Protocol*,IEEE National Conference on Communications (NCC),2010, CoRR abs/1001.2140:2010.

[18] M. Fossorier, M. Mihaljevi, H. Imai, Y. Cuiz, K. Matsuura. *A Novel Algorithm for Solving the LPN Problem and its Application to Security Evaluation of the HB Protocol for RFID Authentication*. Lecture Notes in Computer Science, vol. 4329, pp. 48–62, Dec. 2006.

[19] J. Carrijo, R. Tonicelli, H. Imai, and A. C. A. Nascimento, *A Novel Probabilistic Passive Attack on the Protocols HB and HB+, IEICE Trans-*

*actions*, pp. 658–662, 2009.

[20] A. Blum, A. Kalai and H. Wasserman, *Noise-Tolerant Learning, the Parity Problem, and the Statistical Query Model*, Journal of the ACM, vol. 50, no. 4, pp. 506–519, July 2003.

[21] H. Gilbert, M. Robshaw, and H. Sibert, *Active attack against HB+: A Provably-Secure Lightweight Authentication Protocol*, IEE Electronics Letters, vol. 41, no. 21, pp. 1169–1170, Oct. 2005.

[22] K. Ouafi, R. Overbeck, and S. Vaudenay, *On the Security of HB♯ against a Man-in-the-Middle Attack*, in Proceedings of ASIACRYPT 2008, ser. LNCS, vol. 5350. Springer, 2008, pp. 108–124.

[23] J. Katz and A. Smith, *Analyzing the HB and HB+ Protocols in the Large Error Case*, Available from http://eprint.iacr.org/2006/326.pdf.

[24] P. Chose, A. Joux and M. Mitton, *Fast Correlation Attacks: An Algorithmic Point of View*, EUROCRYPT2002, Lecture Notes in Computer Science, vol. 2332, pp. 209–221, 2002.

[25] E.R. Berlekamp, R.J. McEliece, and H.C.A. van Tilborg, *On the Inherent Intractability of Certain Coding Problems*, IEEE Trans. Info. Theory, vol. 24, pp. 384–386, 1978.

[26] A. Blum, M. Furst, M. Kearns, and R. Lipton, *Cryptographic Primitives Based on Hard Learning Problems*, CRYPTO '93, Lecture Notes in Computer Science, vol. 773, pp. 278–291, 1994.

[27] D. Wagner, *A Generalized Birthday Problem*, CRYPTO '02, Lecture Notes in Computer Science, vol. 2442, pp. 288–304, 2002.

[28] J. L. Massey and S. Serconek, *A Fourier Transform Approach to the Linear Complexity of Nonlinearly Filtered Sequences Advances in Cryptology*-CRYPTO 94, Springer, pp. 322–340, 1994.